1154 Shenandoah Village Dr
PO Box 1990
Waynesboro, VA 22980

VIA ECFS

To: Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W., Suite TW-A325
Washington, DC 20554

NTELOS
1154 Shenandoah Village Drive
Waynesboro, VA 22980
Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2016 covering the calendar year ended December 31, 2015.

Date filed: March 1, 2016

This Certification applies to the following affiliated companies (collectively "NTELOS," or "Company").

NTELOS Companies	499 Filer ID
Virginia RSA 6 LLC (includes Richmond 20MHz, LLC)	807081
Virginia PCS Alliance, L.C.	816030
West Virginia PCS Alliance, L.C.	818784
NTELOS Licenses, Inc.	828588
The Beeper Company	807821

Name of signatory: Brian J. O'Neil

Title of signatory: Executive Vice President, General Counsel, Secretary of NTELOS

Certification:

I, Brian J. O'Neil, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The Company has not received customer complaints in the past year concerning the unauthorized release of CPNI in the past year.

Signed 

Attachments: ACCOMPANYING STATEMENT EXPLAINING CPNI PROCEDURES
SUMMARY OF CUSTOMER COMPLAINTS

ACCOMPANYING STATEMENT EXPLAINING CPNI PROCEDURES

This statement accompanies the Company's Customer Proprietary Network Information ("CPNI") Certification for the year ended December 31, 2015, as required by Section 64.2009(e) of the Federal Communications Commission's ("FCC") rules, for the purpose of explaining how the operating procedures of the Company ensure compliance with part 64, Subpart U of the FCC's rules. *See* 47 C.F.R. § 64.2001 *et seq.* The below procedures are specifically designed to comply with the Commission's CPNI rules and regulations, as well as to maintain the security of the CPNI of the Company's customers.

All subsequent references to rule Sections refer to rules under Part 64, Subpart U unless indicated otherwise.

1. **Operating Procedures**

Changes to Account Information

Pursuant to Section 64.2010 (f), when a customer's account information or password has been modified, the Company immediately sends a text notification to the customer's phone number notifying him or her that a change has been made to the account, and that the customer should call customer care with any questions. If such customer is unable to receive a text message or, if the Company receives a reply that the message could not be delivered, the Company mails a postcard to the customer's address of record.

Customer Initiated Calls

Customer care representatives are trained that in order to discuss call detail or other CPNI during a customer initiated phone call, customers must first be properly authenticated by providing a password meeting the requirements of Section 64.2010(b). In the event a customer forgets his/her password, the Company has implemented password back-up authentication procedures in compliance with Section 64.2010(e).

In-Store

Employees in Company's retail locations are instructed that no CPNI may be provided to any customer unless the customer presents a valid photo ID for authentication pursuant to Section 64.2010(d).

Online Access to Account Information

The Company provides customers with online access to customer account information for which the Company has initiated procedures to control access in compliance with Section 64.2010(c) comprising of authentication through a password meeting the requirements of Section 64.2010(e).

2. **Training Procedures**

Company has established procedures to train employees having access to, or occasion to use customer data. Employees are trained to identify CPNI, consistent the definition of CPNI under Section 64.2003(g) and Section 222(f)(1) of the Communications Act of 1934 as amended (47 U.S.C. § 222(f)(1)). Likewise, employees are trained on safeguards to protect CPNI and as to when they are and are not authorized to use CPNI. Training occurs at the time of hire and again on an annual basis.

In addition, the IT department periodically updates the Company's computer use policy that establishes prohibitions on use and access to CPNI, which every employee must read and sign. All employees have access to CPNI resources and guidelines located on Company's intranet in the event they have additional questions about CPNI and CPNI related issues.

3. **Supervisory Review**

At this time Company does not use CPNI for outbound marketing purposes that requires either opt-out or opt-in consent. Before undertaking to use CPNI for outbound marketing purposes that require such consent, Company will establish a supervisory review process to ensure compliance with Section 64.2009(d).

4. **Customer Notification and Authorization Process**

The Company does not currently use CPNI for marketing purposes that require either opt-out or opt-in consent in accordance with the Commission's rules and thus, at this time, has not provided notice regarding customer ability to opt-out. Prior to any use of CPNI for marketing that requires opt-out consent, the Company would initiate the notification and opt-out process. The Company does not use or disclose CPNI for any purpose that would require opt-in consent and thus does not currently utilize an opt-in approval process. The Company has trained employees regarding prohibitions on use of CPNI for marketing. Prior to initiation of any program for the use of CPNI for marketing purposes, except as allowed under the Commission's rules, the Company will train employees with a need and/or responsibility for obtaining customer authorization to use CPNI for marketing purposes, regarding the notice and approval requirements under Section 64.2008.

5. **Recordkeeping of Use of CPNI**

The Company keeps records of marketing campaigns that use CPNI that includes a description of each campaign, the CPNI used as part of the campaign, and what products or services were offered. As mentioned above, the Company currently does not utilize an opt-out or opt-in consent process. At such time as the Company may initiate use of CPNI for marketing that requires consent (either opt-in or opt-out) with corresponding launch of a notification and opt-out or opt-in process, the Company will develop and utilize a system for maintaining readily accessible records including, but not limited to:

- Whether and how a customer has responded to opt-out approval as required by Section 64.2009(a) or has opted in;
- Company marketing and sales campaigns that use customers' CPNI that requires consent (both Opt-in and Opt-out);
- Instances of where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI.

6. **Disciplinary Process**

The Company has in place an express disciplinary process to address any unauthorized use of or access to CPNI. Employees are notified that any infraction involving CPNI will result in disciplinary action up to and including termination of employment.

7. **Procedures for Notifying Law Enforcement of CPNI Security Breaches.**

The Company has adopted procedures to comply with Section 64.2011 for notifying law enforcement of CPNI security breaches, together with related recordkeeping and deferred notification to customers. If an incident or customer complaint appears to involve CPNI, a designated CPNI point-person within the Company is notified. The point-person will analyze the situation, maintain a detailed

report, and inform law enforcement if necessary pursuant to §64.2011. The point-person also maintains records of incidents pursuant to Section 64.2011(d).

8. **Actions Taken Against Data Brokers and Reponses to Customer Complaints.**

No actions were taken against data brokers in 2015.

The Company received no customer complaints concerning the unauthorized release of CPNI in 2015.